



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 26 January 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- FOX News reports a security guard at a BASF Corp. chemical plant in Freeport, TX, was shot in the shoulder Saturday, January 24, after he approached a suspicious truck and talked to a man who had been taking pictures. (See item [2](#))
- The Tampa Bay Business Journal reports Florida Agriculture and Consumer Services Commissioner Charles H. Bronson has warned consumers of a growing scam in Florida in which sophisticated thieves intercept the numbers on credit cards being used at gas pumps at primarily large service stations. (See item [7](#))
- The Post and Courier reports that days after boxcars filled with bombs, ammunition, and rocket motors derailed in a North Charleston train yard, local and state officials still were struggling to determine exactly what went wrong and what procedures should have been followed in response. (See item [9](#))
- The New York Times reports a World Health Organization official says new tests indicate that the avian flu, spreading in Asia, appears resistant to one of the two main classes of drugs used to fight flu viruses. (See item [20](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector



Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 22, The Guardian (UK)* — **Power blackouts likely again in U.S. Two groups of researchers have independently brought forward evidence of intrinsic weaknesses in the North American power grid. They both conclude that blackouts, such as that in New York last summer, are likely to happen again.** John Kappenman, from a small scientific company in California, last week told the American Meteorological Society in Seattle, WA, that geomagnetic storms could cause larger blackouts. **The Sun ejects streams of charged particles that can warp the Earth's magnetic field, producing atmospheric effects such as the aurora borealis and inducing direct current in transformers. This causes electrical surges, because the grid is meant to take only alternating current.** Separately, Réka Albert of Pennsylvania State University modeled the network, in part to work out why the system failed. The exact cause of the breakdown has not been pinned down, but they conclude that the grid is a so-called "exponential network" which mostly functions without giant hubs to connect large sections. The few well-connected hubs are crucial to power distribution. If transmission substations that bear the highest loads are the first to break down, failure of 4% of them leads to the break-up of about 60% of the network, they report on a physics Website.
Source: <http://www.guardian.co.uk/life/dispatch/story/0,12978,112812,1,00.html>

[\[Return to top\]](#)

Chemical Sector

2. *January 24, FOX News* — **Getaway gunman shoots chemical plant guard. A security guard at a BASF Corp. chemical plant in Freeport, TX, was shot in the shoulder Saturday, January 24, after he approached a suspicious truck and talked to a man who had been taking pictures, authorities said. The guard told police the gunman was a man of Middle Eastern descent with bushy hair and a mustache. The man was driving a white pickup with tinted windows and a black stripe.** Shortly after the incident, local police searched the area with a canine unit and found gun power on the scene, as well as the bullet used in the shooting. The suspect left after the shooting and did not get inside the plant. The guard had been patrolling the plant's perimeter outside the gate and near a water tower but in view of the plant's ammonia tank, officials said.
Source: <http://www.foxnews.com/story/0,2933,109407,00.html>
3. *January 23, Press Enterprise (Catawissa, PA)* — **More chemical spraying alleged.** The McAdoo, PA, man who recently sprayed a chemical mixture from his car in Mifflin Township was charged in a similar incident in New York, police said. Charles J. Lucarelli may have also been involved in other spraying incidents near Danville and Hazleton. Lucarelli, 57, sprayed a liquid from his car in the parking lot of the Red Roof Inn near Danville in late fall, said South Centre Township Police Chief Bill Richendrfer. The hotel manager who witnessed the spraying thought the liquid came from a faulty radiator in Lucarelli's car, Richendrfer said. After seeing news accounts of the January 11 incident near Mifflinville, the manager called police, the chief said. **At Kreiser Truck Stop along Route 339 that day, Lucarelli sprayed Michael and Trudy Bennett's car with a mixture of paint thinner and rubbing alcohol from a spray system rigged in his car's trunk, police said. The incident set off a hazardous material and**

terrorism scare. The next day, police found another chemical mixture and spray system in the car. The second liquid contained ammonia, paint thinner and rubbing alcohol, police said. Police also received reports of similar incidents in the Hazleton and McAdoo areas, said Richendrfer.

Source: <http://www.pressenterpriseonline.com/280882487617886.bsp>

[\[Return to top\]](#)

Defense Industrial Base Sector

4. *January 23, Washington Post* — **Biodefense agency urged for safety of U.S. troops. The Pentagon has not developed a single new vaccine against biological agents since the 1991 Gulf War and should create a new biodefense agency to respond to the growing threat of biological attacks on U.S. forces, according to a congressionally mandated report released Thursday, January 22. The report, by the Institute of Medicine and the National Research Council of the National Academy of Sciences, concludes that the Department of Defense's (DoD) existing biodefense efforts are underfunded and fragmented and offer "dismal prospects for successful results." DoD said in a statement that it is "evaluating the recommendations" of the report and "generally agree[s] with many of them." The department has already taken steps to improve its efforts, it said, including consolidating the chemical-biological defense program, establishing a "military vaccine office" and collaborating with other federal agencies. "We are committed to doing what is required to ensure protection of the health and well being of our troops," the statement said.**

Source: <http://www.washingtonpost.com/ac2/wp-dyn/A40119-2004Jan22>

5. *January 22, Reuters* — **U.S. missile shield will work, Pentagon agency says. The Pentagon agency building a U.S. missile shield on Thursday, January 22 reaffirmed its position concerning the effectiveness of the system. "We believe the system will be reliable and effective against a near-term threat, and will continue to improve over time," said Rick Lehner, spokesperson for the U.S. Missile Defense Agency. President Bush, fearful of possible attacks from nations like North Korea, has ordered fielding of a limited missile defense despite criticism from some experts that it will not be reliable and that it is being rushed into deployment. Up to ten anti-missile interceptors -- six in silos at Ft. Greely, AK, and four at Vandenberg Air Force Base, CA -- are to be part of the initial setup, a supposed bulwark against, first and foremost, any missile attack from North Korea. The Pentagon has planned to spend about \$50 billion over the next five years to develop and field the shield, which would include land-, sea- and space-based sensors and long- and short-range interceptors among other weapons.**

Source: http://biz.yahoo.com/rf/040122/arms_missile_usa_1.html

[\[Return to top\]](#)

Banking and Finance Sector

6. *January 23, Associated Press* — **Government shuts down Website in scam probe. Federal investigators are seeking the source of a phony e-mail purportedly from the Federal**

Deposit Insurance Corp. (FDIC) that asks recipients to click on a Website and provide personal bank account information. FDIC spokesperson David Barr said Friday, January 23, the bogus Website was shut down when the agency was alerted by consumers who received the e-mail. FBI and FDIC officials are investigating who set up the scam. The e-mail says a person's bank account may have been used in violation of the Patriot Act, the anti-terrorism legislation passed by Congress shortly after the September 11, 2001, terrorist attacks, and that the investigation was being conducted with the Homeland Security Department. **The e-mail says that unless that person clicks on the Internet link, the account's federal deposit insurance will be canceled, records will be sent to the FBI for analysis and the owner may receive a visit from Homeland Security.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A42725-2004Jan 23.html>

7. *January 23, Tampa Bay Business Journal (FL)* — **Thieves targeting credit cards at gas pumps.** Florida Agriculture and Consumer Services Commissioner Charles H. Bronson warned consumers on Friday, January 23, of a growing scam in Florida in which sophisticated thieves intercept the numbers on credit cards being used at gas pumps at primarily large service stations. **Bronson said that the thieves attach what is known as a skimming device — a tiny computer-like device the size of a cigarette lighter — to the credit card reader at the pump. While there is no interruption in pumping gas or getting a receipt for the charge at the pump, the skimming device records and stores the unwitting consumers credit card number for later use.** The stolen numbers then can be downloaded onto a computer and be encoded on counterfeit cards.

Source: <http://tampabay.bizjournals.com/tampabay/stories/2004/01/19/daily32.html>

[\[Return to top\]](#)

Transportation Sector

8. *January 25, Chicago Daily Herald* — **Traffic delays at crossings would be expensive to fix.** On a typical day in DuPage County, outside Chicago, trains cause motorist delays of eight to 43 minutes at the county's 25 most congested rail crossings. With Chicago as the nation's rail hub, trains aren't going to stop screaming through the suburbs. **To keep traffic moving, the best alternative might be overpasses and underpasses.** "We want to be a little bit more proactive as a region in garnering the funds for quiet zones," said John Loper, principal transportation planner for the county. To make sure federal money gets funneled the county's way, officials have studied all 163 of the county's railroad crossings to find inaccuracies in the Federal Railroad Administration's train delay intersection rankings and identify places overpasses would work. By showing how an overpass could decrease traffic delays and reduce accidents, officials hope to bump local projects up the consideration list for federal money. "We do have limited resources," said Lanny Wilson, chairman of the DuPage Railroad Safety Council. "Eventually, we are going to engineer all of DuPage County (railroad crossings). But we have to start somewhere."

Source: http://www.dailyherald.com/dupage/main_story.asp?intID=38011 31

9. *January 25, The Post and Courier (Charleston, SC)* — **Derailment turns focus to procedure.** Days after boxcars filled with bombs, ammunition, and rocket motors derailed in a North Charleston train yard, local and state officials still were struggling to determine exactly

what went wrong and what procedures should have been followed in response. The derailment, which occurred at Bennett Yard at 8:20 p.m. Thursday, January 22, resulted in no injuries, but it has raised concerns that notification procedures were not followed and that local authorities and the freight company involved would not be prepared in the event of a terrorist attack. First responders and officials from CSX Transportation, the rail company whose cars derailed, have given conflicting reports of when phone calls were made to authorities and have not been able to establish clearly which group is responsible for transmitting word of such a mishap. Chief Robert Stewart, head of the State Law Enforcement Division and state adviser to the federal agency, will begin discussions with federal Homeland Security representatives and CSX on Monday, January 26, to establish exactly how the derailment occurred and what needs to be done in the future in terms of transmitting information to local police, fire, and ambulance services.

Source: http://www.charleston.net/stories/012504/loc_25train.shtml

10. *January 25, Las Vegas Review–Journal (NV)* — **Banned items seized at airport.** Federal screeners at Las Vegas' McCarran International Airport confiscated nearly 4,500 "deadly or dangerous weapons" at security checkpoints in the 18-month period ending October 31, according to federal records obtained by the Review–Journal last week. **On average, Transportation Security Administration (TSA) workers at the airport collected explosives about every three weeks, a gun every two weeks and a box cutter every day.** "It's not unique to McCarran," said Nico Melendez, a spokesman for the TSA in Los Angeles. "We have found over eight million prohibited items nationwide since February 2002." The records show that scissors were by far the most confiscated item at the nation's eighth-busiest airport. McCarran screeners took 77,497 pairs, or about one pair every 10 minutes. Although more rigid rules about what can be taken on airliners have been in effect for more than two years, travelers using McCarran do not appear to be learning them. **Between April 2002 and last October, TSA screeners at the airport collected an average of about 1,800 prohibited items each week. "Right now, we're doing about 2,800 to 2,900 items a week," Jim Blair, federal security director at McCarran, said Friday, January 23.**

Source: http://www.reviewjournal.com/lvrj_home/2004/Jan-25-Sun-2004/news/23030889.html

11. *January 23, Associated Press* — **Washington, DC considers regulating transport of hazardous materials.** Washington, DC Council members are considering whether to place restrictions on hazardous cargo that is transported through the city. The Committee on Public Works and the Environment is conducting a hearing Friday, January 23, at 2 p.m. Council members Carol Schwartz, David Catania and Kathy Patterson are co-sponsors of the city's **Terrorism Prevention and Hazardous Materials Transportation Act. If the measure is approved, shippers could be forced to obtain special permits, use specific routes and move the cargo during limited hours.** Members of Greenpeace, the Sierra Club, and Friends of the Earth drew attention to the issue last year by pointing out that such cargo travels through portions of downtown on tracks that belong to CSX. **Hazardous cargo is also transported through some areas of the city by truck.**

Source: <http://www.wjla.com/news/stories/0104/120941.html>

12. *January 23, Associated Press* — **Airline industry to work on privacy issues.** Major airlines agreed Thursday, January 22, to work with the Department of Homeland Security on ways to

protect traveler privacy, a difficult new problem as the government seeks to use passenger information to keep terrorists off planes. **Nuala O'Connor Kelly, Homeland Security's privacy officer, met with top airline executives and said they will meet with the department again to discuss privacy protections for their passengers.** "They seemed receptive to the idea that we need to work on and improve privacy policies and to explain the information sharing necessary," Kelly said. Airlines support the government's plan to test a computerized aviation security system that compares passenger information with commercial databases and government watch lists. At issue is how the passenger data will be treated.

Source: <http://www.cnn.com/2004/TRAVEL/01/23/bi.passenger.screening.ap/index.html>

[\[Return to top\]](#)

Postal and Shipping Sector

13. *January 23, Associated Press* — **FedEx to use USPS for new delivery option. FedEx Corp. plans this year to offer a new package delivery service that uses the U.S. Postal Service (USPS) for the final leg.** The product is intended for companies like Internet retailers that mail lots of packages to lots of addresses, said spokesman Jess Bunn. FedEx will likely begin offering the slower, cheaper delivery method in May or June. The new service extends a three-year partnership with the U.S. Postal Service. Currently, FedEx operates some express flights for the USPS, and FedEx has drop boxes at many U.S. Post Offices.

Source: <http://www.miami.com/mld/miamiherald/business/7782538.htm>

[\[Return to top\]](#)

Agriculture Sector

14. *January 24, Australian Associated Press* — **Thailand, Cambodia confirm bird flu. Thailand and Cambodia have confirmed bird flu outbreaks, bringing the number of Asian nations hit by the virus to six.** Avian influenza also has swept through South Korea, Japan, Vietnam, and Taiwan, infecting millions of chickens. "The spread of bird flu is taking on a large-scale regional dimension," said He Changchui, the Asia-Pacific chief of the UN Food and Agriculture Organisation. **The Thai government ended days of denial and admitted it was battling an outbreak of the virus that is devastating its billion-dollar chicken industry.** Tests showed that the disease was present in its poultry population. The European Union, Japan, Singapore, the Philippines, and other nations banned imports of chicken from Thailand, which is among the world's top five poultry exporters. **Scientists have reached no firm conclusions on why the disease is spreading so quickly, but a leading theory is its adaptability,** said Robert Webster, who researches animal viruses for the World Health Organization.

Source: <http://www.theage.com.au/articles/2004/01/24/1074732631933.html>

15. *January 23, Associated Press* — **USDA finds herdsmates of mad cow animal in Idaho. Three cows from an imported Canadian herd that included a mad cow disease-infected Holstein have been traced to a dairy farm in Burley, ID, the U.S. Department of Agriculture (USDA) says.** One of the cows already died, while two others are alive. The Iowa Department

of Agriculture placed a hold order on the farm where they were found to prevent any animals from leaving, Nolan Lemon, a USDA spokesman, said Thursday. State Veterinarian Clarence Siroky announced earlier that a dairyman in Burley had purchased one cow from the Canadian herd in late 2002. The animal became sick last March 18 and died March 23. Siroky said the cow didn't have mad cow disease, formally known as bovine spongiform encephalopathy. The one calf of the now-deceased cow had while in Idaho was stillborn, Siroky said. Neither was slaughtered for food. The other 5,000 cows in the farmer's herd were physically inspected on Wednesday, January 22, and background information on all of them was forwarded to investigators.

Source: http://www.quicken.com/investments/news_center/story/?story=NewsStory/dowJones/20040123/ON200401230927000342.var&column=P0DFP

16. *January 23, USAgNet* — **USDA will update biotechnology rules. The U.S. Department of Agriculture (USDA) intends to update and strengthen its biotechnology regulations for the importation, interstate movement, and environmental release of certain genetically engineered organisms.** USDA's Animal and Plant Health Inspection Service will prepare an environmental impact statement evaluating its biotechnology regulations and several possible regulation changes, including the development of a multi-tiered, risk-based permitting system to replace the current permit/notification system, along with enhancements to the deregulation process to provide flexibility for long term monitoring. Any proposed changes to the regulations will be science and risk-based. The notice was published in the January 23 Federal Register.

Source: <http://www.usagnet.com/story-national.cfm?Id=79&yr=2004>

17. *January 23, Agriculture Online* — **New pork traceability options.** A novel application of DNA analysis that can trace product back to live animals could launch a new era of sophistication in pork traceability, according to Canadian industry leaders speaking at a pork seminar. The industry can't claim to have traceability unless it has complete traceability. If there is product in the meat chain from one producer who does not have sows in the database, then the plant through which that producer markets doesn't have true traceability. The DNA option could provide a missing link in overall traceability. **Analyzing a sample of meat DNA could allow processors to track the meat back to the mother of the animal. That information, if linked to a national live animal tracking system, would allow virtually instant access to animal source and movement.** Pilot tests for the DNA system will be launched this year.

Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail_ANewsindex_html_51225_1

[[Return to top](#)]

Food Sector

18. *January 25, Xinhua News* — **Mobile food safety monitoring facilities. China has developed its first mobile food safety monitoring facilities for fast checking of chemical residues and other harmful substances on vegetables and fruit.** Li Changjiang, director of the State Administration for Quality Supervision and Quarantine, said the facilities will provide a useful tool for quality supervision officials to monitor food safety and protect consumer health. **The new facilities can be used at fruit and vegetable wholesale markets, purchasing and**

processing stations, supermarkets, and on farms.

Source: http://english.eastday.com/epublish/gb/paper1/1158/class0001_00022/hwz178937.htm

19. *January 24, Associated Press* — **Feed manufacturers violate state, federal rules.**

One-fourth of Colorado feed manufacturers have violated state and federal rules designed to prevent the spread of mad cow disease since 1998, according to by the Colorado Department of Agriculture. Many of the violations at the 27 firms cited involved failure to properly label animal feed containing meat and bone meal, or MBM, rendered from the remains of slaughtered cattle. Without such a label, the risk is higher that someone could inadvertently feed the MBM back to cattle, the primary way mad cow disease is transmitted. Other violations include failing to keep proper records of who purchased MBM. Such information would be critical for regulators trying to track down where a cow might have contracted the disease should a case emerge in Colorado or elsewhere. In all, state agriculture officials have repeatedly inspected the just over 100 feed manufacturers in Colorado since mid-1998, a year after the federal government banned the use of MBM for cattle feed.

Source: <http://www.9news.com/storyfull.aspx?storyid=23517>

[[Return to top](#)]

Water Sector

Nothing to report.

[[Return to top](#)]

Public Health Sector

20. *January 25, New York Times* — **Avian flu resistant to a main flu-fighting drug.** New tests show that the avian flu that is spreading in Asia appears resistant to one of the two main classes of drugs used to fight flu viruses, a World Health Organization (WHO) official, Klaus Stöhr, said Saturday. **Knowing that anti-influenza drugs may be needed in an outbreak of human bird flu, and as part of the surveillance process, laboratories in the network have been testing which of a small number of such drugs may be effective against the A(H5N1) strain. Stöhr said that on Friday night his agency learned that initial genetic tests showed that the A(H5N1) was resistant to the less expensive class of anti-influenza virals.** Earlier studies by Malik Peiris of the University of Hong Kong showed that the resistance results from a change in just one of the many amino acids in the avian influenza virus. Additional tests are expected to be conducted this week to confirm the early findings, said Stöhr. A(H5N1) is believed to be susceptible to the costlier class of anti-influenza drugs known as the neuraminidase inhibitors.

Source: <http://www.nytimes.com/2004/01/25/health/25BIRD.html>

21. *January 23, New York Times* — **Avian flu in humans spreads to Thailand. Thai officials announced on Friday that two boys had contracted avian influenza, and six more people were suspected of having it.** The acknowledgment by Thai officials confirmed that the disease was spreading across Southeast Asia and raised fears of a possible global epidemic if the virus mutates into a form that can be passed from person to person. Vietnam has confirmed five fatal

cases near Hanoi and is testing additional suspected cases around the country. **Thai officials say they are testing four more possible cases.** The World Health Organization warned this week that if someone became infected with the bird flu and the human flu at the same time, a mutation could occur that could spread quickly among people. All three of the big influenza epidemics of the 20th century are believed to have started in birds, and the H5N1 strain now killing chickens across East Asia and infecting some people in Southeast Asia is especially lethal.

Source: <http://www.iht.com/articles/126281.htm>

22. *January 23, Associated Press* — **CDC: 2003 West Nile outbreak largest yet. Last year's outbreak of West Nile virus was the largest yet, but fewer people died or had serious brain damage from it compared to 2002,** federal officials said Friday. The 9,006 cases of the mosquito-borne virus in 2003 were more than double the 4,156 cases in 2002, although officials at the U.S. Centers for Disease Control and Prevention (CDC) said the larger number of cases may reflect more testing. CDC officials still consider 2002 to be the worst year for the U.S. because of 284 deaths and 2,944 cases of severe brain damage. Last year, 220 people died and 2,695 suffered severe neurological disease, the CDC said. The agency has already begun preparations for this year's season and is sending money to state health departments to help track the virus and educate people on how to avoid getting infected. The 2003 outbreak revealed holes in health preparations. Even in hard-hit areas, people still were reluctant to take protective measures. **Officials still don't know why the disease erupts in some areas yet leaves others unscathed.** Chicago had large outbreaks in 2002 yet hardly any last year.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=541&ncid=751&e=5&u=/ap/20040123/ap_on_he_me/west_nile_virus

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

23. *January 24, The Post and Courier (Charleston, SC)* — **Derailment spawns new safety concerns. CSX Transportation boasts that it is "obsessed with safety," but Thursday's derailment of a train carrying munitions through North Charleston has renewed concerns about use of the company's tracks to haul a 770-ton defunct nuclear reactor. Though the cause of the January 22 derailment is under investigation, some suggest that an intensive review of CSX's procedures and equipment is in order before the reactor is allowed to travel the railway's track.** The Navy has cleared a North Charleston dock operator to accept the decommissioned reactor after it is shipped 11,000 miles from its current home near San Diego. It would then be sent by rail to a low-level nuclear waste site in Barnwell, SC. No date has been set for the shipment. "That, in my opinion, would put a big stress on the railroad track," said Tom Clements, a senior adviser for Greenpeace's nuclear campaign. "The last thing you want is a ... nuclear reactor dumped out along the railroad tracks in Charleston." CSX

maintains that it is one the safest rail carriers in the country. **"Safety is one of the core values of our company,"** said CSX spokesman Gary Sease. The railway, however, has not been without high-profile failures in meeting its safety goals.

Source: http://www.charleston.net/stories/012404/loc_24safety.shtml

24. *January 22, Free Lance Star (Fredericksburg, VA)* — Virginia Firefighters need equipment.

Most Virginia fire departments cannot supply breathing gear and portable radios for all on-duty firefighters, and only a small percentage have fitness programs even though cardiac arrest is the leading killer of firefighters, a state survey found. The Department of Fire Programs surveyed the state's 599 fire departments last fall, and 431, or 72 percent, responded. **The department's report said it is an "absolute necessity" for firefighters to have access to self-contained breathing apparatus when battling fires, but noted that "only those Virginia departments serving the largest populations [are] currently able to provide SCBA for all responders on duty."** Another safety device used by firefighters is the personal alert safety system that was developed to help rescuers find lost, trapped or injured firefighters. The report also said that many firefighters in Virginia have not received formal training in handling hazardous material events, despite federal requirements for such training dating back more than 20 years. Nearly 20 percent of Virginia fire departments that respond to Hazmat incidents have no one certified "at the most basic awareness competency level," said the report, calling the findings "especially problematic given the increasing threat of terrorism."

Source: http://www.freelancestar.com/News/FLS/2004/012004/01222004/1_239956

[\[Return to top\]](#)

Information and Telecommunications Sector

25. *January 23, Federal Computer Week* — NIST releases telnet, IT security drafts. Federal agencies desiring to minimize work disruptions from outside intrusions can begin with simple safeguards, such as preventing unauthorized users from using the telnet protocol to gain access to a server, according to officials at the National Institute of Standards and Technology (NIST). **Draft documents on computer security released Thursday, January 22, by the NIST give an example of how unauthorized telnet users simply identify themselves as a guest to gain access to sensitive government files.** The Risk Management Guide for Information Technology Systems suggests that disabling telnet is about a 10-hour procedure. Practical advice in the 58-page document includes other ways that agencies can develop standards for safeguarding sensitive but unclassified information in federal computer systems. As applied to information systems, the guide says, risk management is a responsibility of executive managers to be shared with technical managers, and not a technical manager's sole responsibility. Engineering Principles for Information Technology Security, a 33-page document also released this week, offers an overview of accepted principles and practices for security information technology systems. Additional information can be found on the NIST Website:

<http://csrc.nist.gov/publications/drafts.html>

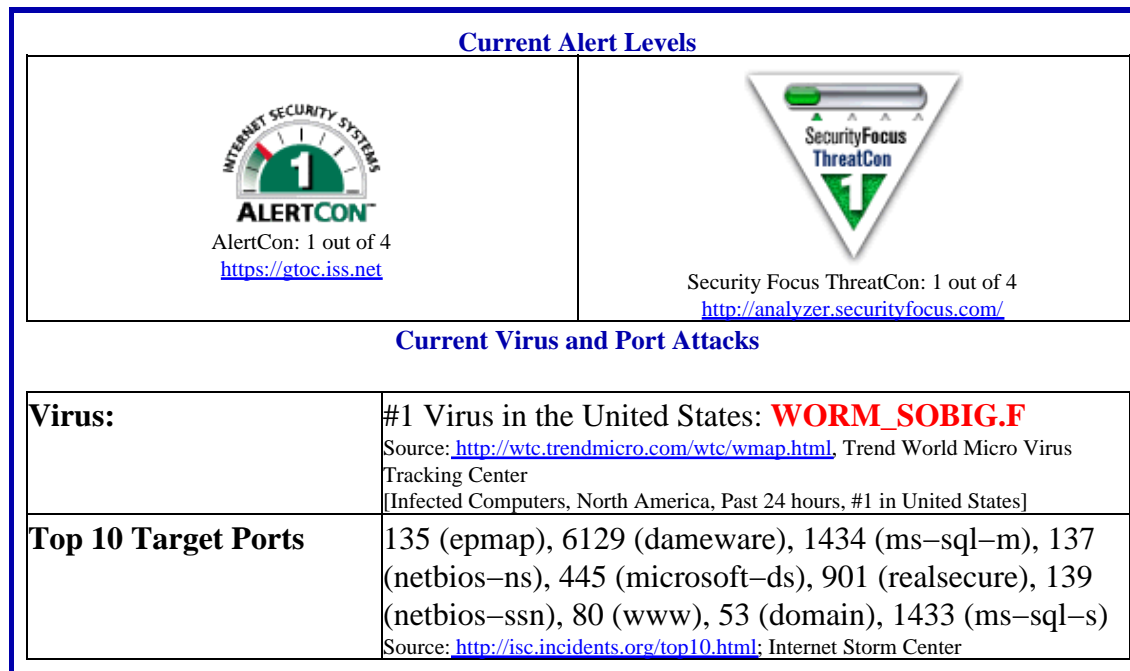
Source: <http://www.fcw.com/fcw/articles/2004/0119/web-nist-01-23-04.asp>

26. *January 22, CNET News.com* — Security pros question flaw find. Two Internet software developers who said they have uncovered a way to cause entire networks of computers to freeze or shut down may have simply rediscovered an old network issue. The network

performance issues are described in a series of Web site forum postings recently publicized within the security community. The poster, who uses the alias NT Canuck, said he created a tool, with the help of another developer, that can shut down entire networks. **However, security researchers at the Computer Emergency Response Team (CERT) Coordination Center downplayed the issue, saying that the program simply inundates a network with so much data that computers have problems functioning correctly.** "We don't see any specific vulnerability being discovered here," said Jason Rafail, an Internet security analyst at the center. According to the Web posts, the programmers found that certain circumstances could be created that would cause a network of computers to freeze, and in some cases fail. The developers contacted Microsoft and the CERT Coordination Center; both organizations confirmed that they were contacted in November. However, Microsoft's Security Response Center (MSRC) has not been able to replicate the discoverers' exact findings, said Stephen Toulouse, senior program manager for the MSRC.

Source: http://news.com.com/2100-7355_3-5145863.html?tag=nefd_top

Internet Alert Dashboard



[\[Return to top\]](#)

General Sector

27. *January 25, CNN* — **Pakistan arrests two senior Taliban officials. Pakistani authorities arrested two senior officials from Afghanistan's deposed Taliban regime Saturday, including one who may know the whereabouts of Taliban leader Mullah Mohammed Omar, Pakistani intelligence sources said. One was identified as Maulvi Abdul Mannan, Governor of Badghais province under the Taliban. He was close to Omar. Also, Najeeb Ullaha, a Taliban military commander, was arrested Saturday. Separately, Pakistani Information Minster Sheikh Rashid said a DNA analysis determined that a leading al Qaeda figure,**

Abdur Rehman Khadar, was killed in a raid by the Pakistani army in October. Eight al Qaeda members were killed in that raid, in a tribal area northwest of Pakistan, the information ministry said. The names of the others were not released.

Source: <http://edition.cnn.com/2004/WORLD/asiapcf/01/24/pakistan.taliban/>

28. *January 24, New York Times* — **Trafficking in nuclear arms called widespread.** The head of the United Nations' watchdog agency on atomic weapons said Friday, January 23, that the illicit trafficking of nuclear-related material and equipment had grown so widespread that it amounted to a supermarket for weapons-seeking countries. Mohamed ElBaradei, the director-general of the International Atomic Energy Agency, said he was taken aback during a recent trip to Libya by the scale and complexity of the black market, through which Libya obtained material and blueprints for nuclear weapons designs. "All of that was obtained abroad," ElBaradei said in an interview during the World Economic Forum meeting in Davos, Switzerland. **"When you see things being designed in one country, manufactured in two or three others, shipped to a fourth, redirected to a fifth, that means there's lots of offices all over the world," he continued.** ElBaradei's confidence, however, was leavened by his acknowledgment that neither the atomic energy agency nor the intelligence branches of the big countries have a grip on the extent of nuclear trafficking. For many experts who have gathered in Davos, nuclear proliferation is looming as the next big security threat.

Source: <http://www.ihf.com/articles/126423.html>

29. *January 24, Associated Press* — **Fingerprint reportedly found at I-71 scene in Ohio.** As he headed home from work along I-71, Michael Thomas saw a person standing on an overpass in front of a parked car. Seconds later, he heard a loud sound and the passenger side of his windshield was cracked. In his rearview mirror, Thomas could see the large four-door sedan on the overpass speed away. Authorities said yesterday the gunshot that struck Thomas' Chevrolet Corsica at about 12:45 a.m. Thursday, January 22, is the 20th in a series of shootings that started in May, 2003. **Thomas said investigators told him they recovered a fingerprint and two shell casings on the I-71 Lambert Road overpass south of Columbus near the Pickaway County line, but a task force investigating the shootings refused to confirm that account.** The shooting sent a fresh wave of fear through the Columbus area because it occurred 7 1/2 miles south of the I-270 south outer belt, where most of the shootings have occurred. **The shooter has fired into an empty elementary school, houses, and at two school buses, forcing one of the region's largest school districts to close for two days before the December holiday break.** The shootings include one fatality: the November 25 death of Gail Knisley, a Washington Court House resident. Police said they would increase marked and unmarked patrols along I-71 in southern Franklin County.

Source: <http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20040124/NEWS03/101240156>

[[Return to top](#)]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883-3644

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.